Information Assurance Metrics Highlights

Dr. Michael Schildcrout

Naval Security Group

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE**	**3. REPORT TYPE AND DATES COVERED**

4. TITLE AND SUBTITLE Information Assurance Metrics Highlights	**5. FUNDING NUMBERS**
6. AUTHOR(S) Schildcrout, Michael	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Naval Security Group	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT *(Maximum 200 Words)*

14. SUBJECT TERMS IATAC Collection, information assurance, metrics, vulnerability analysis, penetration testing	**15. NUMBER OF PAGES** 17
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UNLIMITED

Outline

- Metrics Development Process
  - Joint Service Effort
  - DOT&E Sponsorship
- Risk Levels
- Remaining Issues

Information Assurance Metrics for Operational Test & Evaluation

- Metrics for IA OT&E must be:
  - Physically observable
  - Measurable
  - Quantitative, when feasible
- Directly related to overall goal:

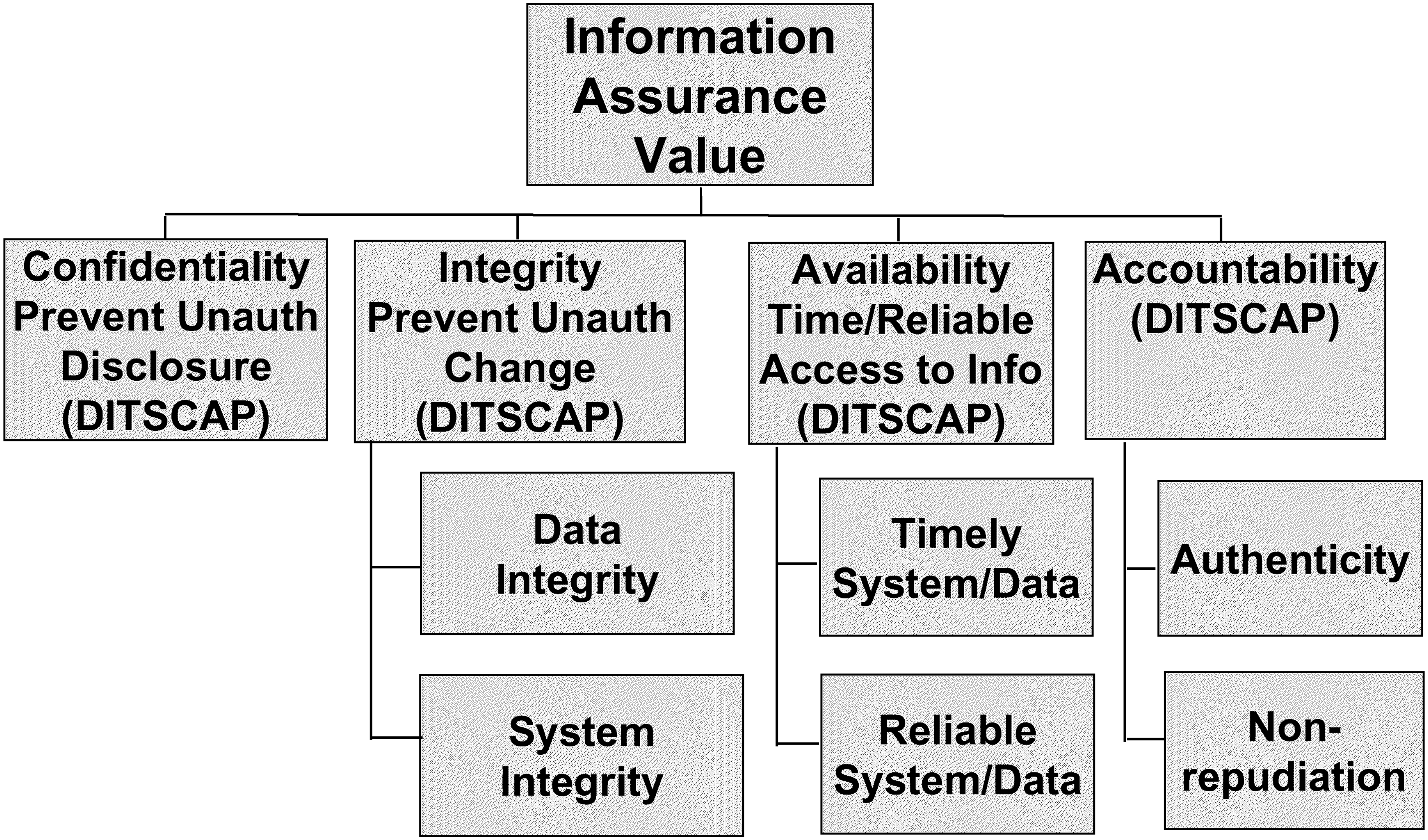
<u>Protection of Information</u>

DITSCAP

DoD Information Technology Security Certification and Accreditation Process

- Developed by the DT Community
- Four Phases. Each phase contains a stage of vulnerability assessment
  - Phase 1: Definition
  - Phase 2: Verification
  - Phase 3: Validation
  - Phase 4: Post-Accreditation

IA Metric Components



Information Assurance Value

Confidentiality Prevent Unauth Disclosure (DITSCAP)

Integrity Prevent Unauth Change (DITSCAP)

Data Integrity

System Integrity

Availability Time/Reliable Access to Info (DITSCAP)

Timely System/Data

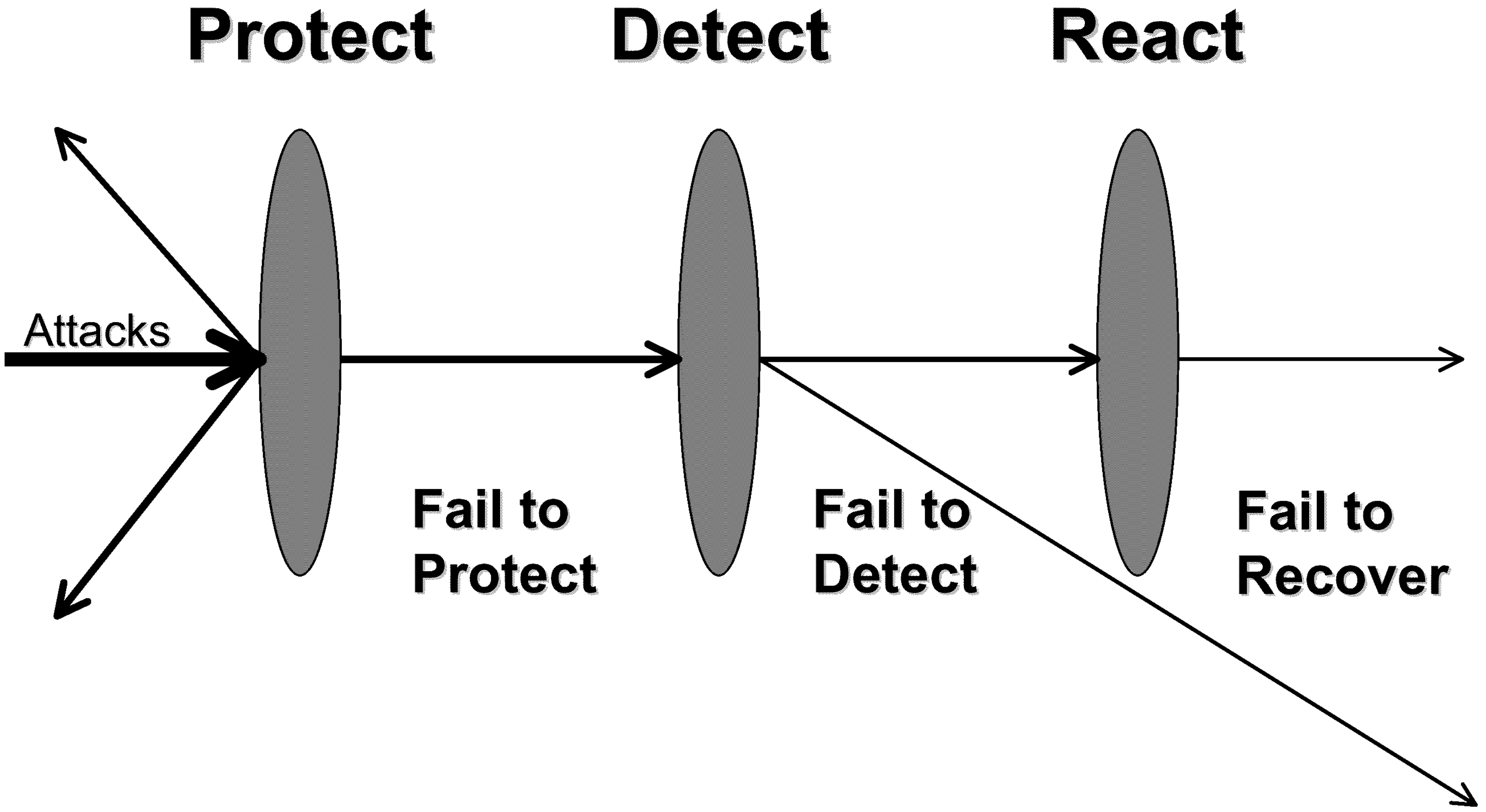
Reliable System/Data

Accountability (DITSCAP)

Authenticity

Non-repudiation

Information Assurance Value



Protect

Detect

React

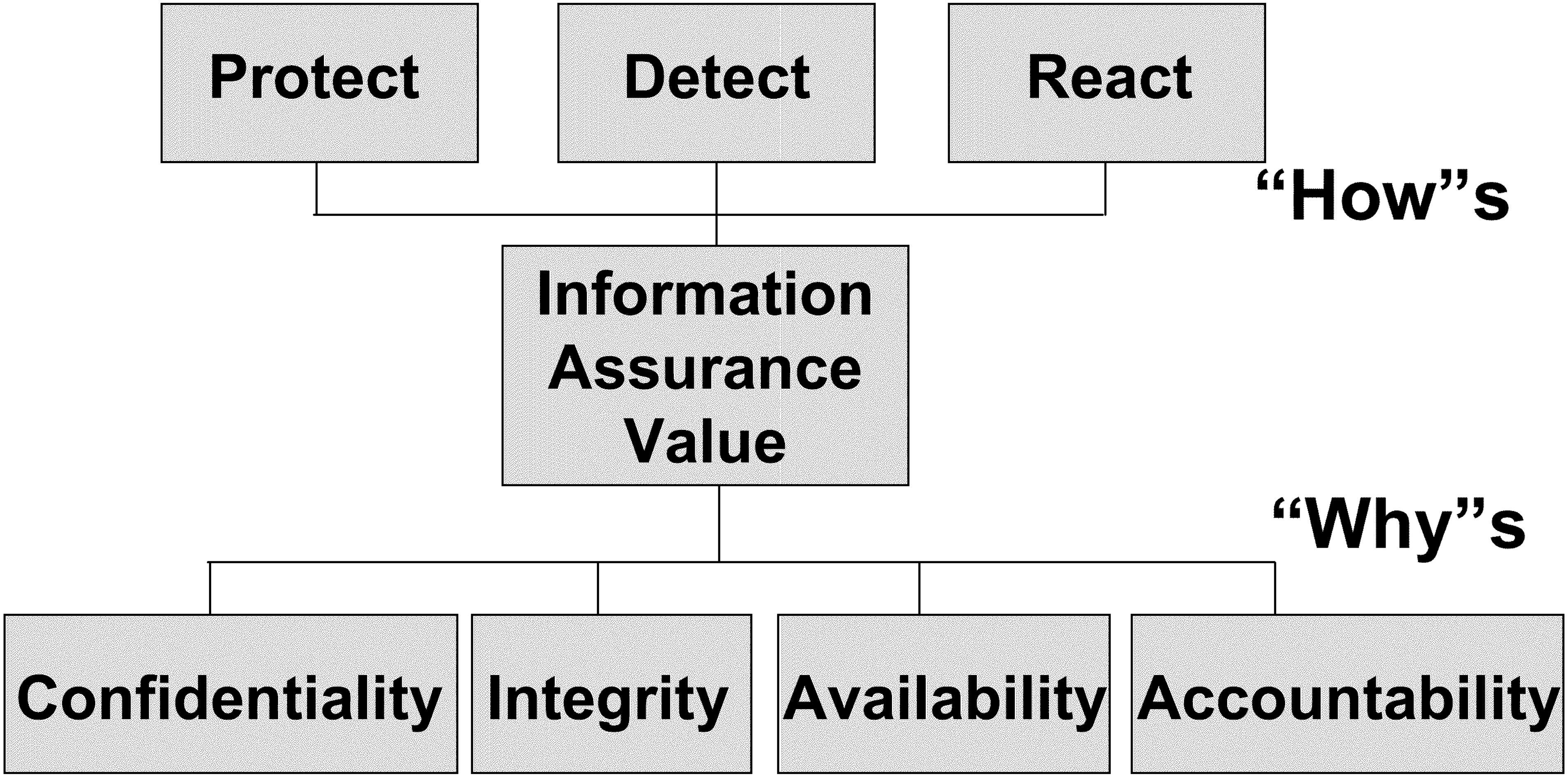
Attacks

Fail to Protect

Fail to Detect

Fail to Recover

“Why”s to “How”s


Protect
Detect
React
“How”s
Information Assurance Value
“Why”s
Confidentiality
Integrity
Availability
Accountability

Streamlined Metrics

1. Review / Inspection of Security Policy
2. Effectiveness against Unauthorized Access or Disclosure
3. Effectiveness against Attack on Data
4. Effectiveness against Attack on System
5. Effort to penetrate to a given level of Access (Privileged, Root, etc.)
6. Effectiveness of Authentication

IA OT&E Test Standards

- Review / Inspection of Security Policy and Procedures
- System Scans
- Penetration Tests
  - Insider
  - Outsider
- Password Cracking
- Detection/Recovery Time

Threat-Risk Assessment Matrix

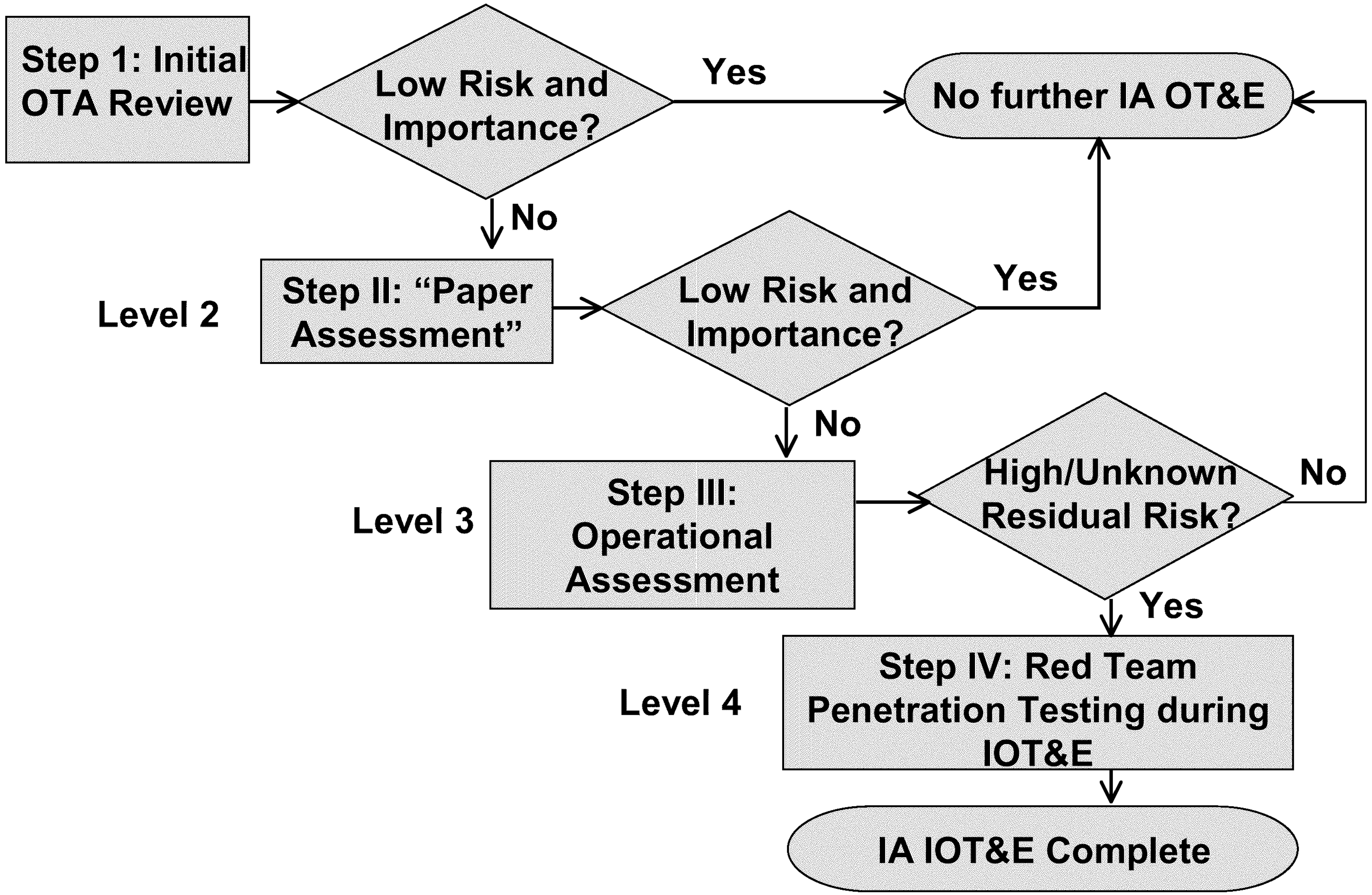
(Higher Level = Higher Risk)

Threat Impact	Likelihood of Threat Penetration		
	Low	Medium	High
Low	Level 1 (None)	Level 2 (Low)	Level 3 (Moderate)
Moderate	Level 2 (Low)	Level 3 (Moderate)	Level 4 (High)
Severe	Level 3 (Moderate)	Level 4 (High)	Level 4 (High)

IA OT&E at the Different Risk Levels

- Level 1
  - Exempt from further testing
- Level 2
  - Paper Assessment based on system documentation. Similar in scope to DITSCAP Phase 1 vulnerability assessment
- Level 3
  - System level assessment similar in scope to DITSCAP Phase 2 vulnerability assessment
- Level 4
  - Similar in scope to DITSCAP Phase 3 vulnerability assessment (Level 3 plus Red Team penetration tests)

IA Process with Risk Levels



Step 1: Initial OTA Review

Low Risk and Importance?

Yes

No further IA OT&E

No

Level 2

Step II: "Paper Assessment"

Low Risk and Importance?

Yes

No

Level 3

Step III: Operational Assessment

High/Unknown Residual Risk?

No

Yes

Level 4

Step IV: Red Team Penetration Testing during IOT&E

IA IOT&E Complete

Remaining Issues

- How complete are the metrics?
  - There will always be the need for flexibility
- How often must IA OT&E be repeated?
- How can compatibility with DITSCAP be improved?
- Which organization(s) will maintain the IA database?
  - What will be the format?
- Others?

Back-ups

IA OT&E Metrics

1A. Effectiveness of security policy in preventing unauthorized access: all test standards met?

1B. Effectiveness of system's defense in depth: all test standards met?

2A. Effectiveness of system in preventing unauthorized access (Insider and Outsider): acceptable or not acceptable?

2B. Effectiveness of system in preventing unnecessary disclosure of system information: acceptable or not acceptable?

3A. Ability to detect information degradation/corruption/attack: acceptable or not acceptable?

3B. Time (thresholds set by the user) to respond to information degradation/corruption

3C. Time (threshold set by the user) to restore degraded, corrupted information

4A. Ability to detect system degradation/corruption/attack: acceptable or not acceptable?

4B. Time (threshold set by the user) to respond to system degradation/corruption.

4C. Time (threshold set by the user) to restore critical functionality in a degraded, corrupted system

4D. Time (threshold set by the user) to restore full functionality in a degraded, corrupted system

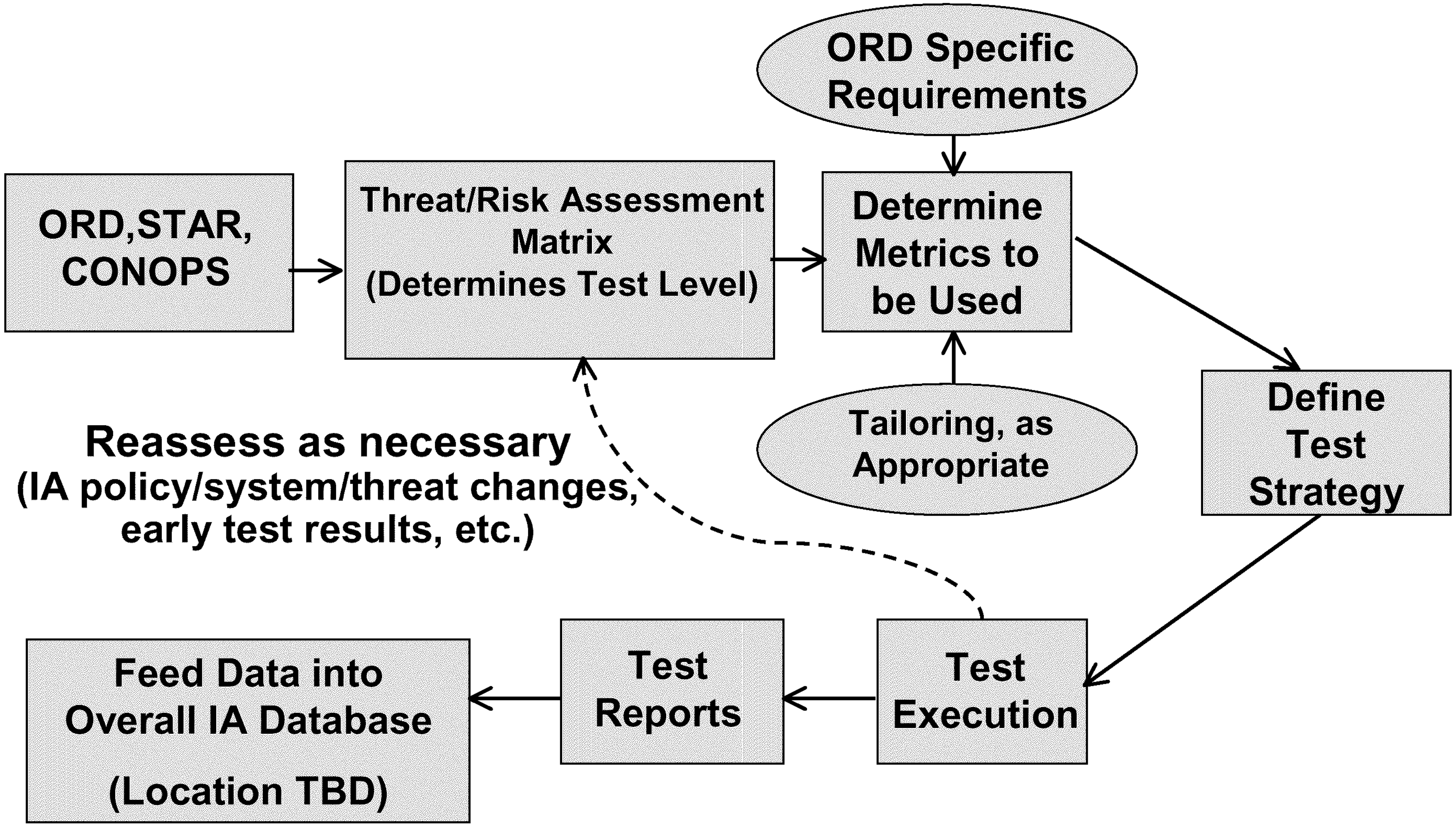
5. Effort (low, medium, high) to penetrate to a given level of access

6. Effectiveness of authentication?

Example IA Metric with Test Standards

IA OT&E Metric	Test Standard
2A. Effectiveness of system in preventing unauthorized access (from both Insider and Outsider): acceptable or not acceptable?	• System Test - for low risk/low impact systems only • Vulnerability Analysis / Penetration Test - all others (as required; degree TBD; Inside and Outside) • List severity of Known Vulnerabilities; none, low, medium, or high
2B. Effectiveness of system in preventing unnecessary disclosure of information; acceptable or not acceptable?	• System Test - for low risk/low impact systems only • Vulnerability Analysis / Penetration Test - all others (as required; degree TBD)

IA Operational Test Level Process



ORD,STAR, CONOPS

Threat/Risk Assessment Matrix (Determines Test Level)

ORD Specific Requirements

Determine Metrics to be Used

Tailoring, as Appropriate

Define Test Strategy

Reassess as necessary (IA policy/system/threat changes, early test results, etc.)

Test Execution

Test Reports

Feed Data into Overall IA Database

(Location TBD)